HOGAN & HARTSON
L.L.P.

DAVID L. MARTIN

DIRECT DIAL
(202) 637-5858

February 6, 2006

Marlene Dortch, Secretary
Federal Communications Commission
445 Twelfth St., SW
Washington, D.C. 20554

> **RE: EB-06-TC-060**
> **EB Docket No. 06-36**
> **SunCom Wireless, Inc.**
> **Certification of CPNI Filing (February 6, 2006)**

Dear Ms. Dortch,

In response to the Commission's public notice DA 06-223 (released Jan. 30, 2006), SunCom Wireless, Inc. hereby submits its most recent officer certification and explanatory statement, executed pursuant to 47 C.F.R. § 64.2009(e), confirming compliance with the Commission's customer proprietary network information ("CPNI") rules.

Respectfully Submitted,

/s/ David L. Martin

David L. Martin
Hogan & Hartson L.L.P.
555 13th Street N.W.
Washington, DC 20004
(202) 637-5600
(202) 637-5910

Counsel to SunCom Wireless, Inc.

cc: Byron McCoy
        Best Copy & Printing

CERTIFICATION OF COMPLIANCE
WITH CUSTOMER PROPRIETARY NETWORK INFORMATION RULES

I, Charles Kallenbach, Senior Vice President Legal and Regulatory of SunCom Wireless,

Inc. ("SunCom"), hereby certify that I have personal knowledge that SunCom has established

operating procedures that are adequate to ensure compliance with the rules of the Federal

Communications Commission, set forth at 47 C.F.R. § 64.2001 *et seq.*, regarding the use of

customer proprietary network information ("CPNI"). The attached Explanatory Statement

describes such compliance.

Charles Kallenbach
Senior Vice President Legal and Regulatory
SunCom Wireless, Inc.
1100 Cassatt Road
Berwyn, PA 19312

Dated: February 6, 2006

SunCom Wireless, Inc.
Explanatory Statement Regarding CPNI Compliance
February 2006

As described below, SunCom Wireless, Inc. ("SunCom") has long-established procedures to protect the confidentiality of customer proprietary network information ("CPNI") pursuant to Section 222 of the Communications Act of 1934, as amended, and to ensure compliance with the FCC's CPNI rules (47 C.F.R.§§ 64.2001-64.2009). In addition to its existing procedures, SunCom has recently alerted its employees to media reports of "data brokers" who attempt to obtain customer data from carriers through fraudulent means. In light of these reports, SunCom has reminded its employees of the importance of strictly following the company's customer verification procedures prior to releasing CPNI to any person.

- SunCom provides only CMRS and associated CPE and information services. SunCom does not use CPNI to market any services outside of its single service category. Therefore, under the "total services approach," the opt-in and opt-out procedures for customer approval delineated in §§ 64.2007 – 64.2008 of the FCC's rules are not applicable to SunCom, as SunCom does not market any services to its customers other than those to which the customer already subscribes.

- SunCom does not disclose or permit access to CPNI by third parties for the marketing of any non-SunCom service, and SunCom itself does not use CPNI to market any services provided by third parties.

- Any CPNI released to independent contractors is protected from further disclosure through the use of confidentiality agreements. For example, SunCom's contract with its data processing vendor prohibits the vendor from using the CPNI for any purpose not specifically contemplated by SunCom, and requires the vendor to undertake the necessary measures to safeguard the CPNI against unauthorized disclosure, misuse, espionage, loss and theft. The vendor must protect the CPNI from unauthorized disclosure to any person or entity and must advise all of its employees, subcontractors and similar individuals of their obligation to protect the CPNI. (These provisions satisfy § 64.2007(b)(2)'s requirements for confidentiality agreements.)

- Internally, SunCom has established policies and procedures to safeguard CPNI:
  - Access to CPNI is on a "need to know" basis only. For example, retail sales associates do not have access to CPNI.
  - As part of a supervisory review process governing the use of CPNI, employees must receive permission from their supervisors before using or disclosing CPNI for sales or marketing purposes.
  - Employees must follow established company procedures for customer account verification prior to releasing CPNI to any person.
  - Improper access, use, treatment or disclosure of CPNI may result in disciplinary action up to and including termination of employment.

- SunCom has established a mandatory employee training program on the proper use of CPNI. As part of the training, employees are provided with a document entitled "CPNI 101" which explains CPNI and SunCom's policies regarding the proper use and safeguarding of CPNI, as summarized above. Employees must acknowledge that they have read the training document.

- In addition, all employees must affirmatively acknowledge, on an annual basis, that they have received and agree to abide by SunCom's Professional and Business Code of Conduct, which is incorporated as part of the employee handbook. The Code of Conduct explicitly states that:
  - o All customer information, which includes CPNI, must be maintained in the strictest of confidence, and that it may not be disclosed except as authorized and necessary when performing duties for SunCom.
  - o Improper use or unauthorized disclosure of the information may result in the initiation of legal proceedings, as well as disciplinary actions.
  - o This obligation is a condition of employment and continues in effect even after employment with SunCom ceases.

- SunCom maintains records, for at least one year, of its sales and marketing campaigns in which CPNI is used. These records identify the CPNI used and the products and services offered.

- Beyond the specific requirements of the CPNI rules, SunCom undertakes other precautions that further minimize the potential for unauthorized access to CPNI, including an electronic data retention policy under which historical billing information is removed from the central customer database after a certain period of time.